تحقيق

تريز الخوري
khourytherese@hotmail.com

الذكاء الإصطناعي في لبنان من يحمي أجيالنا من الفضاء الرقمي؟

يشهد العالم تطورا تقنيا متسارعا ينعكس على مختلف جوانب الحياة، من العمل والتعليم إلى التواصل وتبادل المعلومات. وعلى الرغم من إسهام الوسائل الحديثة في تسهيل المعاملات وتوسيع آفاق المعرفة وتشجيع الابتكار، فإنها تفرض تحديات مرتبطة بصون الخصوصية والحماية الإلكترونية والحد من الأخبار الكاذبة، مما يتطلب ترسيخ ثقافة الاستخدام الآمن والمدروس

نواجه مرحلة مفصلية تفرض علينا مواكبة التحولات التكنولوجية والاستفادة من الفرص التي يتيحها الذكاء الاصطناعي، الذي لم يعد مجرد أداة مساعدة، بل أصبح عاملا مؤثرا في أساليب الإنتاج والتفاعل. ومع اتساع استعماله في مختلف المجالات، تبرز الحاجة إلى رؤية وطنية تحدد كيفية توظيفها، بما يخدم التنمية، يعزز الابتكار، ويفتح آفاقا جديدة أمام المؤسسات والشركات والأفراد. لا تقتصر أهميته على ذلك فقط، بل تمتد إلى تأثيره المباشر في المجتمع، لا سيما في حياة الأطفال والمراهقين الذين باتوا أكثر انخراطا في البيئة الرقمية. فمن جهة، تتيح هذه الامور فرصا للتطوير وتسهيل الوصول إلى المعرفة، تحفيز الإبداع وتنمية المهارات، ومن جانب آخر تثير تحديات تتعلق بسلامة المحتوى، حماية البيانات الشخصية، وانتشار التزييف العميق، كما أن الاعتماد المفرط على هذه الأدوات الذكية، قد يضعف القدرة على التفكير النقدي والتحقق من الاشياء. من هنا، تبرز ضرورة تحقيق التوازن بين الاستفادة والحد من المخاطر، من خلال تدريب الجميع، ووضع أطر قانونية ورقابية تضمن الخصوصية ومساءلة الجهات المعنية عن إساءة الاستعمال.



"الأمن العام" حاورت وزير الدولة لشؤون التكنولوجيا والذكاء الاصطناعي كمال شحادة، والرئيس التنفيذي للمعلوماتية وأمن المعلومات في شركة "تاتش" حسن دهيني.

شحادة: نعمل لتطوير القوانين ومواكبة المستجدات

■ إلى أي مدى يشكل الذكاء الاصطناعي ضررا على الاجيال؟

□ لا يمكن القول إنه يشكل خطرا في ذاته على الاولاد قبل بلوغ سن الرشد، بل تتوقف مخاطره على طبيعة المحتوى الذي يتعرضون له، ومدى وعيهم على كيفية التعامل معه. فعلى الرغم من الفوائد الكبيرة التي توفرها هذه التكنولوجيا في مجالات التعليم والمعرفة وتنمية المهارات، إلا أن الاستعمال غير المسؤول لها قد يؤدي الى مجموعة من المشاكل، من بينها الوقوع تحت تأثير المضمون غير الملائم لأعمارهم، الاستغلال، انتهاك الخصوصية، سرقة البيانات الشخصية، فضلا عن الصور والفيديوهات المفبركة التي يمكن إنتاجها باستخدام التقنيات المتطورة، والتي قد يصعب عليهم التمييز بينها وبين ما هو حقيقي. كما أن الاعتماد المفرط عليه، قد يؤثر في قدرتهم على التفكير النقدي والتحليل والتحقق من الامور، ويجعلهم أكثر عرضة لتصديق الأخبار غير الموثوق بها، لذلك تبرز أهمية الحماية، والمساعدة من دون الحرمان من الفوائد. نجري حاليا نقاشات لمواكبة التطورات المتسارعة في هذا المجال، في ظل التحديات الجديدة التي تفرضها هذه الامور، والحاجة إلى وضع آليات واضحة للتعامل معها. إن المطلوب حاليا، أن تتضافر الجهود لأن المسؤولية لا تقع على جهة واحدة، بل هي مشتركة تستدعي المتابعة المستمرة والتعاون بين جميع المعنيين. الهدف ليس منع أحد من اللجوء الى التطور، بل علينا تحصين المجتمع من الآثار السلبية التي قد تنجم عن إساءة استخدامه.

■ ما هي أبرز المشكلات التي يواجهها القاصر نتيجة الاستخدام غير المنضبط للتقنيات الذكية ووسائل التواصل؟ ومن يحاسب؟

□ ان الصعوبات التي نواجهها تشمل التنمر الإلكتروني، انتهاك الخصوصية، الاستغلال الرقمي، المضمون غير الصحيح، إضافة إلى الاعتماد المفرط على أدوات هذه التقنيات من دون التحقق من المعلومات. يقع على الأهل أيضا دور التأكد من أن ما يصل إلى أولادهم محدود. فعلى الدولة وضع التشريعات والرقابة، وعلى الشركات توفير بيئة أكثر أمانا، في حين يتوجب على أولياء الامور والصروح التربوية التوعية والتوجيه. إن الهدف ليس إبعادهم عن التكنولوجيا، بل إعدادهم للاستعانة بها، وتعزيز آليات الإبلاغ عن كل ما يدور في فلك الاحتيال، بالتنسيق مع كل المعنيين.

■ كيف يمكن مواجهة الأخبار الكاذبة والمفبركة التي طورتها الانظمة الذكية؟

□ لا يمكن القول إننا نمتلك تشريعات كافية ومتكاملة لمواكبة جميع التحديات التي تفرضها الابتكارات التكنولوجية المتسارعة. نحن نعمل بالتعاون مع وزارة العدل، على عدد من مشاريع القوانين التي تتعلق بالأمن السيبراني وخصوصية المعلومات وحماية البيانات الشخصية، باعتبارها ركائز أساسية لبناء إطار صحيح ومتكامل يواكب التطورات ويحد من المخاطر. كما نسعى من خلال هذه المشاريع إلى صون المواطنين، لا سيما الفئات الأكثر عرضة للمخاطر، في مقدمها أصحاب الاعمار الصغيرة الذين يحتاجون إلى ضمانات إضافية تحميهم من الاخبار الضارة. كذلك نولي أهمية كبيرة لوضع قواعد صارمة، وتحديد مسؤوليات المنصات الرقمية ومساءلتها عند الإخلال بواجباتها، بما يضمن توفير بيئة إلكترونية موثوقة. لكن التحدي لا يقتصر على إصدار الانظمة، بل يشمل أيضا تطوير آليات تطبيقها ومواكبتها للتغيرات المستمرة، وتعزيز التعاون بين كل مكونات المجتمع، إلى جانب نشر الوعي الرقمي لدى الجميع. العالم يتطور بوتيرة سريعة، مما يفرض علينا مراجعة الضوابط بصورة مستمرة، لضمان عدم وجود ثغر يمكن استغلالها للإضرار بالافراد. هدفنا هو الوصول إلى منظومة متكاملة تحقق التوازن بين الاستفادة وحماية الحقوق والخصوصية، وتضمن اعتماد هذه التقنيات بطريقة سليمة مع الحفاظ على كل ما يصل الينا من جديد بعيدا من المخاطر والاستغلال. من المهم اليوم التمييز بين الحقيقي والمزور، كما يجب تعزيز المسؤولية وتشجيع المستخدمين على التحقق من كل معلومة قبل نشرها. فالأولوية هي وضع اطار وطني متكامل يجمع بين التشريعات الفعالة، المساءلة، التوعية، وحماية البيانات الشخصية. هذا لا يتحقق بالحظر وحده، بل ببناء بيئة تمكن الجميع من الاستفادة من التكنولوجيا وتحد من سلبياتها.



وزير الدولة لشؤون التكنولوجيا والذكاء الاصطناعي كمال شحادة.

■ عملت فرنسا على تقييد استعمال وسائل التواصل لمن هم دون 15 عاما، ماذا يمكن للبنان أن يستفيد منها؟

□ تظهر تجربة باريس أهمية وضع ضوابط لحماية القاصرين، ويمكن للبنان استثمار الامكانات لتطوير مقاربة متوازنة تجمع بين التنظيم القانوني والتوعية والرقابة. لقد واجه المنع، بصيغته الأصلية، عقبة دستورية في آب 2026. وهنا استطرد لأقول إن الهدف الاول منذ تسلمي المهام، كان ولا يزال التأسيس للحكومة الرقمية، ووضع الأطر التنظيمية الواضحة والمبادرات الداعمة لقيام اقتصاد متطور وآمن، تقدما للخدمات بطريقة راقية تليق بالناس. كما اعرّف بمبادرة "نمو" التي اطلقناها لتمكين أكبر عدد من الشباب من استعمال التكنولوجيا المتقدمة عبر ورش تدريبية متخصصة انطلقت في مختلف المناطق.

دهيني: التقنيات الذكية لا تغني عن التشريع

■ هل تستطيع شركة touch حظر المواقع أو التطبيقات ذات المحتوى الضار أو غير المناسب للأطفال والمراهقين؟

□ تمتلك الشركة الإمكانات التقنية التي تتيح لها حجب نطاقات ومواقع إلكترونية وعناوين محددة على مستوى الشبكة، بما يحد من الوصول إلى المعلومات المؤذية أو غير المناسبة، بما في ذلك المحتوى الذي قد يعرض الاولاد لمشكلات مختلفة. لكن تنفيذ الحظر لا يتم بقرار منفرد من جانبنا، بل استنادا إلى القرارات والتوجيهات الصادرة عن الجهات الرسمية المختصة، لا سيما القضاء ووزارة الاتصالات ◄

والأجهزة الأمنية المعنية، ووفقا للأطر النظامية والإجراءات المعتمدة. في هذا السياق، من المهم التمييز بين القدرة التقنية على الحجب والصلاحية لاتخاذ القرار في شأنه، إذ تلتزم الشركة تنفيذ التوجيهات الرسمية ضمن نطاق اختصاصها. كما أن التعامل مع المضامين غير المناسبة يتطلب تنسيقا بين الجهات المعنية، إلى جانب تعزيز الوعي لدى الأهل والمراهقين بسلبيات الاستعمال غير الآمن للإنترنت، وتشجيع الإبلاغ عن الاشياء المخالفة أو المسيئة. فتقييد الوصول إلى الامور الخطرة، قد يشكل إحدى الوسائل للحد من ولوج بعض المواقع، لكنه لا يكفي وحده لتوفير حماية شاملة للابناء، خصوصا في ظل تعدد التطبيقات وتطور أساليب النشر، مما يجعل الارشاد الرقمي والمتابعة الأسرية والتعاون المؤسسي عناصر مكملة وأساسية لرعاية المستخدمين الصغار.

■ هل يمكن منع المواد المنتجة تقنيا بهدف الخداع أو الغش أو التهديد؟

□ نحن نتمكن من ايقاف الروابط والمواقع والأرقام التي يثبت استعمالها في هذه الامور غير المشروعة، كمواقع التصيد الاحتيالي والرسائل المشبوهة. يتم ذلك، استنادا إلى معلومات التهديدات الأمنية وأنظمة المكافحة، أما المحتوى المتداول داخل المنصات العالمية فهو مشفر ولا يستطيع مشغل الاتصالات الاطلاع عليه أو تمييزه. لذلك، فان مهمة رصده وإزالته تقع أساسا على عاتق هذه المواقع، بالتعاون مع الجهات الأمنية المختصة، وهكذا يبقى ادراك المستخدم خط الدفاع الأول.

■ هل تستطيعون توفير خدمة رقابة أبوية؟

□ نقدمها عادة وفقا لمستويين: الجهاز كأدوات الإشراف العائلي المتوافرة مجانا في الهواتف وأنظمة التشغيل، وننصح الأهل باستخدامها. اما على صعيد الشبكة، فالخدمة التي يقدمها المشغل تتيح تحديد فئات المواقع والتطبيقات المسموح بها لابنائهم. المنفعة الثانية ممكنة تقنيا، وتدرس "تاتش" إمكانية تقديمها كاختيارية ذات القيمة المضافة، إذا كان المنع دقيقا ومحددا، أي أن يستهدف مواقع أو روابط مصنفة ضارة،


الرئيس التنفيذي للمعلوماتية وأمن المعلومات في شركة "تاتش" حسن دهيني.

استنادا إلى قرار قانوني واضح وأدوات تصفية تعتمد على سمعة القوائم المحدثة باستمرار، لا أن يطال التسهيلات بأكملها. كما أن الحلول الاختيارية تحقق هذا التوازن، لأنها تضع القرار في يد الآباء والمستفيد بدلا من فرض قيود عامة على الجميع.

■ ما هي حدود قدرة شركة الاتصالات على حظر المواقع؟ وهل تحتاج إلى تعاون مع الجهات الرسمية أو شركات التطبيقات؟

□ للحجب على مستوى الشبكة حدود واضحة، فمعظم حركة الإنترنت اليوم مشفرة. كما تتمتع شركات الاتصالات بقدرة على حظر بعض المواقع والمحتويات، لكن هذه القدرة لها نطاق معين، مما يجعل من الصعب التمييز بين محتوى وآخر داخل المنصة الواحدة. كذلك، يمكن الالتفاف على بعض الاجراءات عبر اعتماد الشبكات الافتراضية الخاصة (VPN)، فضلا عن أن اخفاء مادة رقمية كبرى، قد يتعذر من دون الاستغناء عن فضاء رقمي بأكمله، وهو ما قد يحرم المستخدمين من الوصول إلى خدمات مشروعة. لذلك، لا يمكن الاعتماد على التعطيل كوسيلة شاملة للحماية، بل لا بد من التعاون بين كل المعنيين على ثلاثة مستويات أساسية هي السلطات الرسمية التي تتولى وضع الأطر واصدار القرارات المتعلقة بتحديد نطاقها وفقا للانظمة المرعية الإجراء، علما أن مزودي الخدمات والمنصات الرقمية التي تمتلك القدرة على إزالة المضمون المخالف من مصدره، وتعطيل الحسابات التي تنشر، وتطوير آليات الإبلاغ والمراجعة. كما أضيف الى ذلك، الأهل والمدارس، من خلال تعزيز التوعية، ومتابعة استعمال الأطفال والمراهقين للإنترنت، وتعليمهم كيفية التمييز بين المواد. من هنا، لا بد من أن أقول، إن الوقاية الفاعلة تتطلب الجمع بين الإجراءات التقنية والتشريعات الواضحة، بما يضمن الحد من الامور غير المجدية، من دون المساس غير المبرر في حق المستخدمين في الوصول إلى الخدمات المشروعة.

■ هل يمكن استخدام الذكاء الاصطناعي لاكتشاف المضمون المؤذي والحد من انتشاره قبل وصوله إلى المستخدمين؟

□ لقد بات ركيزة أساسية في أنظمة الأمن الفضائي الحديث والمتقدم، فهناك أنظمة لكشف التسلل ومكافحة الاحتيال. تستخدم خوارزمياته لتحليل حركة البيانات ورصد الأنماط المشبوهة، واكتشاف البرمجيات الخبيثة والتصيد الخادع والرسائل الاحتيالية، بشكل استباقي، علما أن الشركة تعمل على تعزيز قدراتها في هذا الاتجاه ضمن منظومتها للحماية الرقمية. أما رصد المواد المنشورة وحذفها، فهي من مسؤولية القنوات الالكترونية في الدرجة الأولى. علما أن التقنيات الذكية تظل أداة مساعدة لا تغني عن الإطار التشريعي والرقابة البشرية والتوعية.

"الذكاء الإصطناعي"... ضوابط vs أخطار



شهد العالم تحولات دراماتيكية نتيجة الذكاء الاصطناعي أو ربما سنعتاد على تسمية جديدة هي "الذكاء الفائق"،(super intelligence- SI)، الذي لم يعد مجرد تقنية متقدمة يجري استخدامها في مراكز الدراسات والأبحاث، بل أصبح واقعا سيرافقنا كالظل بشكل مستدام.

بدأت البحوث الحديثة في هذا المجال في منتصف القرن العشرين، لا سيما بعد مؤتمر "دارتموث" عام 1956، ثم تطورت بصورة تدريجية خلال العقود التالية. إلا أن الانطلاقة الكبرى جاءت مع تطور الحوسبة، وتوافر كميات هائلة من البيانات. فكان التحوّل الكبير عام 2022، حيث ظهرت تأثيراته الإيجابية، ويا للأسف السلبية ايضا، في كل القطاعات ومندرجات الحياة. الطب وتشخيص الأمراض واكتشاف الأدوية، الصناعة والروبوتات ومراقبة الجودة، الزراعة وإدارة المياه والمحاصيل، المصارف وكشف الاحتيال، النقل والطاقة، التعليم والبحث العلمي، الإعلام، الإدارة العامة والأمن السيبراني.

السؤال المطروح هو ما إذا كان الذكاء الاصطناعي سيدخل حياتنا، بل كيف سنستخدمه وبأي ضوابط؟

في وقتنا الراهن، تبرز مخاطر جدية، خصوصا بالنسبة إلى الأطفال، فيما العالم يسعى لدرء اخطاره. ففي أوستراليا فرض التشريع في 10 كانون الأول 2025 قيودا على حسابات وسائل التواصل الاجتماعي لمن هم دون 16 عاما، مع استثناءات للتعليم والصحة والتطوير المهني وغيرها. أما الاتحاد الأوروبي، ففي أيلول 2026، اقترحت المفوضية إطارا جديدا لحماية الأطفال رقميا، يتضمن جعل بعض روبوتات المحادثة ورفقاء الذكاء الاصطناعي مغلقة افتراضيا أمام القاصرين، على أن يتمكن الأطفال من إدارة حسابات التواصل الاجتماعي بأنفسهم بدءا من سن 15.

اما الرئيس الاميركي الأسبق باراك اوباما فقد كان له وجهة نظر مميزة، حملت في طياتها تحذيرا مبطنا من هذه التكنولوجيا بقوله: "لا أعتقد أن هذه التكنولوجيا مبالغ في تقدير أهميتها، فقد اصبحت الآلات قادرة على تعليم نفسها بنفسها. ولم تعد مضطرة إلى انتظار البشر لكي يكتشفوا الأشياء ويعلّموها إياها". وسأل عن مخاطرها، فأجاب: "الخطر الكبير الذي نراه في أفلام الخيال العلمي، أن تصبح هذه النماذج أكثر ذكاء منا، وأن تقرر أن البشر لا مشكلة في وجودهم، لكنهم ليسوا ضروريين. ثم تبدأ بوضع أهدافها الخاصة، وتقوم الروبوتات القاتلة بالقضاء علينا، أو نضطر إلى الخضوع لها، وقد يكون هناك احتمال، ولو كان غير صفري، لحدوث ذلك".

اضاف: "المشكلة الأكثر خطورة هي أن هذه النماذج إذا وقعت في أيدي أشخاص سيئين، قد يستخدمونها للقيام بأشياء سيئة. ويمكن تسليحها أو استخدامها لأغراض ضارة، كما يمكنها أن تسبب الكثير من الأذى والمشكلات".

اذا، الخطر قائم، والخشية أن يتم استغلال الذكاء الاصطناعي من جانب شبكات الجريمة المنظمة والتهريب والاحتيال والهجمات السيبرانية، والتنمر ونشر الشائعات وانتحال الشخصيات والتلاعب بالمعلومات. لكن في الوقت نفسه، الذكاء الاصطناعي له وجه آخر ايجابي، فهو يستطيع كشف الاحتيال، ورصد الهجمات الإلكترونية، واكتشاف المحتوى المزيف، وتحليل العمليات المالية المشبوهة، ومساعدة المؤسسات الأمنية والعلمية والطبية في معالجة كميات ضخمة من المعلومات. لذلك لا يبدو الحل في منع الذكاء الاصطناعي، بل في تنظيمه وضبطه وحسن استخدامه ومنع ذوي الارادات الاجرامية من استثماره. المطلوب تطوير تشريعات تحمي الإنسان، وإلزام الشركات بمبادئ السلامة منذ التصميم، تعزيز حماية البيانات، ووضع ضوابط خاصة لحماية الأطفال، وإبقاء القرار البشري حاضرا في المجالات الحساسة كالطب والقضاء والأمن والتعليم.

التحدي الحقيقي ليس في الذكاء الاصطناعي نفسه، بل في الطريقة التي يختار الإنسان استخدامها. فإذا أحسنّا توجيهه، يمكن أن يصبح أداة هائلة لخدمة العلم والصناعة والتعليم والطب والاقتصاد والأمن. أما إذا تركناه بلا ضوابط، فقد يتحول إلى أداة تضاعف قدرات الجريمة والتضليل والاستغلال.

المبدأ الأساسي في عصر التكنولوجيا الفائقة، هو أن يزيد الذكاء الاصطناعي من قدرة الإنسان لا أن يلغي عقله، وأن يخدم المجتمع لا أن يتحكم به.

"الأمن العام"